האיגוד הישראלי לבטיחות מערכות מידע

THE ISRAELI ASSOCIATION FOR INFORMATION SYSTEMS SECURITY

THE ANNUAL CONFERENCE 1986 הכינוס השנתי

תכנית ותקצירים

מלון הילטון, תל-אביב

22 - 23 בדצמבר 1986

הנהלת הכינוס

ראול פולק - יו"ר הכינוס
ב.מ.ב. בטיחות מערכות בינה

אריה בירון
רתב"ג תעשיות

נסים בראל
אגוד הבנקים

שלמה הנדל
בנק לאומי לישראל

שאול לביא
משרד הבטחון

ששון מרון
בנק דיסקונט לישראל

חוה סלומון
בנק המזרחי המאוחד

כתריאל צימט
יו"ר איל"א

אליעזר תאומי
בנק הפועלים

בצלאל תאזיני
יבמ - ישראל

מזכירות וארגון:

ארטרא בע"מ
רח'קאופמן 2, תל-אביב
ת.ד. 50432, תל-אביב 61500
טל. 03-664825
טלקס 361142

יום ב' 22 בדצמבר 1986

שעה		עמוד התקציר
09:00-08:00	**התכנסות**	
10:30-09:00	**מושב פתיחה** ברכות: ר. פולק, נשיא האיגוד הישראלי לבטיחות מערכות מידע כ. צימט, יו"ר האיגוד הישראלי לעיבוד אינפורמציה י. פויכטוונגר, נשיא לשכת המבקרים הפנימיים בישראל ש. הנדל, נשיא לשכת מבקרי ענ"א	
09:45-09:20	הרצאת אורח כבוד: פרופ' י. באבד, CPA, PHD, אוניברסיטת אילינוי-שיקגו **"בטיחות מערכות מידע מנקודת ראותו של רואה החשבון"**	
10:30-09:45	**"מגמות והתפתחויות בתחום מערכות מידע בנקאיות והשפעתן על בטחון ובטיחות מידע"** ד"ר מ. גוטרמן-עוזר למנכ"ל, מנהל אגף המחשבים, בנק דיסקונט לישראל	4
11:00-10:30	הפסקת קפה	
	מושב א' יו"ר: א. תאומי, מבקר הבנק, בנק הפועלים	
11:45-11:00	**"תכנון אסטרטגי: החוליה החסרה בבטחון מידע"** כ. צימט, יו"ר האיגוד הישראלי לעיבוד אינפורמציה	5
12:30-11:45	**"עקרונות ויישום אבטחת מידע בארגון"** ב. תאזיני, מנהל בטחון, בטיחות ואבטחת מידע, י.ב.מ ישראל	6
14:00-12:30	הפסקת צהרים	
	מושב ב' יו"ר: ש. מרון, (ISR) CPA, CISA, CIA, מבקר ראשי, בנק דיסקונט לישראל	
11:45-14:00	**"פשיעה באמצעות מחשב"** ניצב משנה נ. פליט - אגף החקירות, משטרת ישראל	
15:30-14:45	**"בטיחות מידע במערכות תקשורת"** ד"ר ד. בירן - מנכ"ל c4s ו-מבמ מערכות ממוחשבות	8
16:00-15:30	הפסקת קפה	
	מושב ג' יו"ר: ש. פנירי, סגנית מפקחת על הבנקים, בנק ישראל	
16:45-16:00	**"תפקידי הנהלה וגורמים מקצועיים של הארגון ביישום אבטחת מערכות מידע"** ד"ר ר. גרנות - רפא"ל	15
17:30-16:45	בטיחות העברת כספים אלקטרונית (EFT) **"אבטחת מידע במערכות .S.W.I.F.T"** (SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATION) י. ירום, ראש מטה אגף תפעול, בנק לאומי לישראל	20

יום ג', 23 בדצמבר 1986

שעה		עמוד התקציר
	מושב ד' יו"ר: כ. צימט, יו"ר האיגוד הישראלי לעיבוד אינפורמציה	
09:45-09:00	**"היבטים משפטיים (אזרחיים ופליליים) בהפעלת מערכות מידע ממוחשבות"** עו"ד י. מלכו - חבר הועדה להכנת ההצעה של חוק המחשבים	22
10:30-09:45	**"פונקציות ביקורת בסביבה ממוחשבת, הווה ועתיד"** ש. מרון - CPA(ISR), CISA, CIA, מבקר ראשי, בנק דיסקונט לישראל	24
11:00-10:30	הפסקת קפה	
	מושב ה' יו"ר: ח. סולומון, אגף אשראים, בנק המזרחי המאוחד	
11:45-11:00	יישומי בינה מלאכותית: **"מערכות מומחה: העתיד של בטיחות מערכות מידע"** ר. פולק - מנכ"ל ב.מ.ב., בטיחות מערכות בינה	27
12:30-11:45	**"הביקורת הפנימית ובטיחות המידע"** ש. הנדל - CISA, מנהל ביקורת מערכות מידע, בנק לאומי לישראל	31
14:00-12:30	הפסקת צהריים	
	מושב ו' יו"ר: ד"ר י. בירן, מנכ"ל C4S ו-מבמ מערכות ממוחשבות	
14:45-14:00	**"פתרונות טכנולוגיים באבטחת מערכות מידע"** נ. בראל - איגוד הבנקים בישראל	
15:15-14:45	**"תכנון למצבי חירום"** ד. אמיתי-מהנדסת מערכות, ר.ד.ט הנדסת אלקטרוניקה	33
15:40-15:15	הפסקת קפה	
18:00-15:40	**טכנולוגיות ומוצרים זמינים בישראל בתחום אבטחת המידע** הרצאות מסחריות	

מגמות והתפתחויות בתחום מערכות מידע
בנקאיות והשפעתן על בטחון ובטיחות מידע
=====================================

ד"ר מנחם גוטרמן
בנק דיסקונט לישראל בע"מ, עוזר למנכ"ל, מנהל אגף המחשבים

הפעילות הבנקאית, הידועה בדרך כלל בשמרנותה המופגנת, עוברת בשנים האחרונות שינויים קיצוניים בנהלים והרגלים של עבודתה, בסוגים ובמיגוון של פעילויותיה ובצפיותיהם של מקבלי השרותים שלה (לקוחות).

הירידה ברווחיות מערכת הבנקאות והופעתם של גורמים פיננסיים מתחרים לבנקאות הביאו להגברת התחרות בתחום הבנקאות ובהכרח לחיפוש דרכים למשיכת לקוחות מכל פלחי השוק האפשריים, ליצירת כלים מפתים ולהתיעלות.

דרכים אלה תרמו להתפתחותם המואצת של כלים טכנולוגיים מתקדמים ביותר בתחום מערכות המידע, כאשר תחום הבנקאות משמש להם "שדה נסויים" ושדה יישום מובהק.

באמצעות המאפיינים העקריים של מערכת הבנקאות, אותם נציג להלן, נזהה את המגמות בתחום מערכות המידע:

- רישום מידע באמצעים מקוונים.
- גישה למידע בנקאי בזמן אמיתי.
- הפעלה עצמית של תחנות קצה ע"י הלקוחות.
- בנקאות ביתית ובנקאות עסקית.
- מערכות תומכות החלטה.
- מערכות בינבנקאיות משולבות.
- מערכות משולבות בין בנקים לבין רשתות שיווק ומוסדות פיננסיים.

כל מאפיין מבין אלה שהוזכרו לעיל (ועוד רבים אחרים שלא הוזכרו כאן) מהווה נדבך וציון דרך בהתפתחות מערך עבוד נתונים אוטומטי על כל המשתמע ממנו.

הרצון למתן שרות בזמן אמיתי, למשל, מחייב הקמת תשתית תקשורת רחבת היקף. השאיפה למתן שרות בנקאות ביתית ובנקאות עסקית מחייב הקמתם של מאגרי מידע רכוזיים ויצירת כלים "ידידותיים" למשתמשי הקצה. לכל אחת מפעולות אלה, שצוינו כאן כדוגמאות אחדות מני רבות, השפעה בולטת על בטחון ובטיחות מידע.

יתרה מזאת, כל פעולה כזו מהווה פירצה בחומת הבטיחות (הרופפת למדי) של מערכות המידע הבנקאיות.

כתריאל צימט - בטיחות מערכות מידע

שם ההרצאה: תכנון אסטרטגי, החוליה החסרה בבטחון מידע.

הגישה לבטיחות מידע בעבר היתה גישה של תגובה: פיתוח אמצעי אבטחה ומנגנוני בקרה לאחר מעשה.

כדי להצליח בסביבה הטכנולוגית המתפתחת במהירות יש להתייחס לבטיחות המידע כבר בעת תכנון המערכת הממוחשבת.

דרושה הבנה של שיטות תכנון בהתייחס למטרות האסטרטגיות של הארגון.

ההנהלה והמשתמשים זקוקים להסברה לגבי הפוטנציאל והמגבלות של מנגנוני בקרה. טכנולוגיות חדשות בפתח, מחשבים אישיים חודרים לכל תחומי הפעילות של הארגונים, בסיסי מידע רבים פתוחים לסקירה ואפילו לעדכון ע"י אנשים רבים בארגון.

כל ההתפתחויות הללו מגדילות את הסכנות באשר לשימוש בלתי מבוקר של משאבי המידע. לכן יש להתכונן ולהקדים רפואה למכה.

ההרצאה תתייחס להיבטים שונים של הבעיות ותציע מתודולוגיה מתאימה.

<u>עקרונות ויישום אבטחת מידע בארגון</u>

בצלאל תאזיני
יבמ ישראל בע"מ

זרעי הבעיה השרשית של אבטחת מידע נטמנו באותו רגע שהופעל המחשב הראשון ב-1945 -- MARK I -- באוניברסיטת הרוורד בארה"ב. הניצנים הראשונים נבטו בסוף שנות הששים עם הופעת השימוש בעיבוד מבוזר -- רשתות שתוף-זמן (time-sharing) והאפשרות של רכוז מידע רב במאגרים נגישים בקלות יחסית.

במסווה של "בעיה" הופיעה על הבמה "תת-בעיה" של הגנת הפרטיות(Privacy) שהיא סוגיה חברתית, תחיקתית ומשפטית שהביעה את החשש בציבור מפני איבוד הבקרה על אופן האיסוף, שימוש, העברה, שלימות ומהימנות הנתונים הנוגעים לפרט.

מאידך, תת-הבעיה היא היא שבעצם נתנה הדחיפה והדרבון לקידום הנושא של אבטחת מידע, ראשית ע"י תחיקה הקיימת כיום ברוב מדינות המערב הדמוקרטיות. שנית ע"י פיתוח כלים טכנולוגיים ואחרים בכדי לענות על האתגר של הגנת הפרטיות, שאפשר לסכמו כך:

- נתונים שמותר לאסוף/לאגור
- כיצד לאסוף, להשתמש, להעביר
- מי אוסף, משתמש, מעביר
- איך להבטיח דיוקם ושלימותם
- כיצד לאפשר לפרט לבדוק ולעדכן

אם נמשיך בנמשל ה"חקלאי" בו פתחנו, היום אנו נמצאים בתוך שדה פורח, או אם תרצו יער עבות, כאשר למרות הנסיון הרב שנרכש והספרות המקצועית המצויה, עדיין יש רבים התועים ותוהים איך לתקוף הבעיה וליישם תכנית אבטחה סבירה.

מדי פעם מתרחשים התעוררות והתרגשות עקב דווחים בכלי התקשורת על מקרי חדירה או שימוש לרעה במערכת זו או אחרת, או כאשר מופיעות תקנות מחמירות הכוללות "עונש צפוי של מאסר שנה".

כפי שנראה, מקרי חדירה אלה, אינם הבעיה, והם רק קצה הקרחון; מחקירה די קצרה שלהם, מתברר שאמצעי הגנה פשוטים וטריוויאלים למדי היו יכולים למנעם ורק חוסר-דעת, זלזול ורשלנות השאירו פירצה כה גלויה.

הגישה האיטית או היעדר גישה ליישום אבטחת מידע השורר בדרך כלל, מזכיר נושא טבע אחר, מזג האוויר ש"כולם מדברים עליו" ולא ניתן לשפרו. מטרת מאמר זה להראות שאין האנלוגיה תופסת כלל ועיקר ושאפשר לפעול בצורה משמעותית, סבירה ושקולה בכדי לאבטח המידע ונכסי עיבוד נתונים אחרים.

<u>הגדרת מטרות</u>

על תכנית לאבטחת מידע לספק כלים, אמצעים, שיטות ונוהלים להגנה סלקטיבית של נכסי ענ"א, מידע ונתונים בפני:

- גילוי או שינוי בלתי מורשים
- אבדן

<u>בשגגה או במזיד</u>

לסיכום פרק זה, על מערכת אבטחת מידע לתת מענה לשאלות, כגון:

- רמת הפגיעות של מתקנים לסיכונים
- אמצעים שיש לנקוט על מנת למנוע ולצמצם תוצאות של:
  - אסון
  - הפרעה ממושכת בפעילות ליום, יומיים, שבוע וכו"
  - הונאה, או שימוש לא מורשה, או ניצול לרעה

נסקרים הנושאים הבאים: כימות הבעיה, המציאות בא אנו פועלים וחיים עם המסקנות המשתמעות מהם. אלה מובילים להצגת התנאים המוקדמים ועקרונות ליישום המובאים להלן.

__תנאים מוקדמים ליישום__

- קיום הוראות והנחיות מפורטות בכתב הנתמכות במלואן ע"ל ההנהלה וידועות מובנות ומקובלות ע"ל סגל העובדים.
- מדיניות ברורה וחד משמעית לטיפול בחריגים.
- הגדרת אחריות ותפקידים: מי עושה מה ומתי.
- Control Base המגדיר מרחב ההגנה ותרגומו לפעילויות ספציפיות שאפשר להבין, לעכל ולנהל.
- קיום מודעות והדרכה

__עקרונות ליישום__

- זיהוי וסווג מתאים של כל נכס ומידע על כל מדיה.
- עקביות, המשכיות והתמדה של בקרה ומניעה
- גילוי בזמן מספיק ומתאים של אירועים ותגובה מידית ואפקטיבית.
- חבות אישית (Personal Accountability)
- Least Privileges -- Need-To-Know
- הפרדת רשויות

__סיכום__

האם ניתן ליישם תכנית כזו, לאור ולמרות כל הקשיים שאולי השתמעו בהרצאה.

התשובה היא כמובן כן !

הצעד הראשון הוא נחישות ההנהלה בהחלטה על יישום ותמיכה וגיבוי לצוות שעליו תוטל האחריות על בסיס "זמן מלא" לביצוע לפי הקווים שהוצגו כאן.

בשלב שני, שלב ההקמה הקשה והארוך ביותר, יש להתמקד במיפוי החשיפות הרציניות ביותר ולהכין תכנית פעולה לחיסולן. כאן החוכמה היא להבדיל בין העיקר לתפל ולדעת לתת הקדימויות הנכונות והטיפול המיטבי בכל חשיפה.

הניסיון של אחרים מצוי וכמו כן רבים הכתובים, יש רק לסגלם ולתרגמן בהתאם לסביבה הארגונית הספציפית.

בטיחות מערכות מידע בתקשורת

ד"ר דוד בירן - מנכ"ל C4S ומבם מערכות ממוחשבות בע"מ

תקציר

אנו מצויים בעידן בו מערכות מידע הן יעילות כתוצאה מכך שהמערכות מופעלות בתקשורת וכי מידע הוא מבוזר.
מערכות סגורות מביאות תועלת לאוכלוסיות מעטות ונבחרות. העולם כולו נמצא בבעיה בה מחד, מחוייבת גישה למערכות מידע מכל מקום בעולם, ומאידך, קיימת סכנה אף קיומית לגופים רבים כתוצאה מהפגיעה במערכות ע"י התקשורת.

אין המערכות זהות בייעודן, יש מערכות בעלות פוטנציאל לנזקים כלכליים אדירים כגון מערכות EFT, SWIFT ומערכות אחרות שבהן הנזק עשוי להיות חברתי, בטחוני ואישי.
קיים הכרח לטפל במערכות כאלו בתחילת דרכן עם התכנון.

המאמר מבהיר קונספטים בתחום בטיחות מערכות מידע בתקשורת, בעיות ופתרונות אפשריים.

כללי

מערכות מחשבים והתקשורת אליהן בכל ארגון גורמות להווצרותן של בעיות חמורות בבטחון הנתונים. גישה של גורם בלתי מוסמך לנתונים עלולה לגרום לנזק אדיר למוסד לו הם שייכים והן לפרט אחד או יותר.
רשתות תקשורת הנתונים או האפיקים המוקדשים לתקשורת זו מטופלים מבחינה טכנית באופן דומה לנעשה בטלפוניה. ספק התקשורת מספק למשתמש קו. הקו נותן הגנה סבירה כך שבדומה לנעשה בטלפוניה, בה כאשר מדברים בקו תקין לא שומעים את השכנים, כן גם המצב כאן. כאשר זוג ציודי קצה לנתונים מעבירים בניהם מידע אין המשתמשים צריכים לחשוש כי מישהו יקלוט את המידע בנוסף להם. יש כאן איפוא הגנה על הפרטיות PRIVACY שפרושה שנקטו אמצעים סבירים כך שמושב (SESSION) תקשורת הנתונים לא יועבר לגורמים אחרים כגון ציודי קצה הקשורים בקו מקביל לזה בו מדובר. הגנה כזו מבוססת על תנאים שגרתיים של עבודה ומזג אויר. לעיתים קורה שכאשר קיים מזג אויר גשום או יש תקלה במערכות ניתן לשמוע בטלפון שיחה נוספת אחת או יותר לזו בה מדבר זוג אנשים. דבר דומה ומסיבות דומות יכול לקרות גם בתקשורת נתונים. זוהי פגיעה בלתי מכוונת בפרטיות וההסתברות לכך נמוכה ביותר. בדרך כלל ניתן להניח כי הגורם שעלה בטעות על השיחה לא יעשה שמוש לרעה בה.

במושג בטחון (SECURITY) הכוונה שונה לגמרי. כאן ברור שגורם כלשהו מעוניין לצותת לשיחת הנתונים המועברת. לשם כך הנו מצטייד מראש בציוד שתואם את ציוד המתקשרים ביניהם מבחינת קצב, קוד, פרוטוקול, סוג המודם וכו'. כלומר המצותת חייב להצטייד במערכת תאימה לגמרי לזו אליה הנו מעוניין לצותת. בעיה נוספת העומדת בפניו הינה היכן להתחבר פיזית לגורם המצותת. הדבר הנוח ביותר הוא באחד משני המתקנים ביניהם נעשה הקשר או לאורך המסלול. ציתות מעין זה מחייב מקצוענות, ידע מוקדם והכנה מוקדמת של ציוד וכמובן שיש לכך השלכות כלכליות נכבדות אם כי לגורמים רבים השקעות אלו כדאיות.

אפשרויות טפול בבטחון בתקשורת נתונים

מערכת תקשורת נתונים כלשהיא מוקמת בין שני מקומות פיזיים שונים המתקשרים זה עם זה באמצעות אחד התווכים האפשריים.
חייבים להגן על המתקנים מפני גישה בלתי רצויה ולהגן על הנתונים במחשב עצמו מפני שליפה מקומית על ידי גורם בלתי מוסמך, מכיוון שלהגן פיזית על מסלול תקשורת נתונים שעקרונית יכול להיות ארוך עד אין סוף, זוהי משימה בלתי אפשרית. הרי יש צורך להסתיר את הנתונים כך שגם אם יצותתו אליהם לא ניתן יהיה להבינם. לתהליך זה של הסתרת הנתונים או המרתם לצורה בלתי מובנת קוראים בשם הצפנה ENCRYPTION.
הטקסט המקורי נקרא בשם גלוי (PLAIN או CLEAR).
הטקסט הבלתי מובן נקרא בשם טקסט מוצפן (CIPHER TEXT). תהליך הגלוי החדש של המידע המקורי מתוך המוצפן נקרא בטול הצפנה (DECRYPTION).

ניתן להבטיח בטחון בתקשורת נתונים על ידי :

* נעילת המתקן בו נמצא הציוד ומניעת כניסתם של גורמים שאין תפקידם מחייבם להמצא במקום.

* נעילת המסופים - ניתנת לביצוע ע"י מפתח חיצוני אחד או יותר. כאשר יש לדוגמא שני מפתחות ניתן להקנות לכל מפתח דרגת הרשאה מסויימת.

  כך לדוגמא, הרשאה גבוהה יותר תהיה בידי המנהל אשר יחזיק רק אצלו את המפתח השני. המפתחות עצמם יכולים להיות פיזיים מקובלים, כרטיסים כלשהם ואפילו מפתחות בתכנה.

* שם המשתמש מופיע גם בדרך כלל במדריכים גלויים במגמה לאפשר פניה למשתמשים שונים. לכן, שם המשתמש נשאר בדרך כלל קבוע ואין לסמוך עליו מבחינת שמירה על בטחון.

* החלפה תדירה של סיסמא - לכל משתמש נתונה סיסמא משלו אותה הוא יכול להחליף, אפילו מדי הפעלה. בדרך כלל נוהגים המשתמשים לקבוע את שם הסיסמא בשים לב לשם מסויים (אשה, ילדים וכו'), ולהשאירה בתוקף במשך זמן רב. לדבר זה יש סכנה רבה.

* הוספת שם משתמש וסיסמא נוספים לצרכי טפול בחומר שנקבע כמסווג וזאת לאחר התחברות רגילה באמצעות שם המשתמש והסיסמא הראשונים.

* זהוי המסוף המתקשר על ידי קביעת תשובה אוטומטית (ANSWER BACK). שיטה זו מקובלת במערכות טלקס/טלטקס וכן במערכות בנקאיות.

המגרעת של התשובה האוטומטית היא בכך שהמשתמש מוגבל למסוף מוגדר הנמצא במקום מסויים.

* בקרה על התקשורת - מכתיבים למערכת ליישומים מוגדרים קבלת התקשרות רק ממסופים מוגדרים מסויימים. במידה וקיים נסיון התקשרות של גורם אחר כלשהוא תתקבל התרעה במרכז בקרת הרשת.

* הגבלת משתמשים מבחינת שמוש ביישומים מוגדרים. בתכנית בקרה של היישומים קובעים לאיזה משתמש מותר להגיע לאיזה יישום. הקביעה יכולה להיות חד משמעית או מותנית בקיום תנאי מוגדר.

* קביעת נוהלי עבודה ברורים - המנעות מקיום נוהל עבודה תגרום להתרעה מיידית או מאוחרת יותר. לדוגמא, ניתן להורות את המחשב להודיע למשתמש מתי פנה אליו לאחרונה ובמידה וברור למשתמש שבאותו הזמן לא יכול היה להתפנות, הרי הוא מוזהר.

הצפנת מידע

הצפנת מידע היא האמצעי החשוב ביותר שמבטיח את המידע בזרימתו או באחסונו. ההצפנה יכולה להעשות בחמרה, בתכנה או בשלוב של חמרה ותכנה. ההצפנה יכולה להעשות באמצעות מפתחות (KEYS), הידועים רק למשתמשים המפורשים. ההצפנה יכולה להעשות מקצה לקצה (END TO END ENCRYPTION), או שהיא יכולה להעשות על חלקו של מסלול התקשורת בין צומתי התקשורת. בשנים האחרונות פותחה גם אפשרות של הצפנה תוך שמוש במה שנקרא הצפנה צבורית (PUBLIC ENCRYPTION), בה משתמשים בשני סוגי מפתחות, האחד שניתן לקבלו מתוך מדריך גלוי לצרכי הצפנת מידע ואילו השני נמצא רק בידי המקבל ורק באמצעותו ניתן לגלות מחדש את המידע המקורי. המפתחות בהם משתמשים לצרכי הצפנת המידע מבוססים על שיטות שונות (תלובנה בהמשך) ועל אלוגריתמים שונים. לכל מפתח חוזק משלו.

עקרונית ניתן לאמר, כי כל מפתח אפשר לפרוץ, מותנה במאמץ שמגדירים המתבטא בזמן, בעצמת המחשב בו משתמשים לשבירת המפתח, בהשקעות ובכ"א המשתתף בתהליך. לכן, חשוב להיות מודע כי אין מערכת שנותנת 100% הגנה. לכן, נהוג להגדיר את חזקם של המפתחות במושגים של זמן בטוח יחסית עד לפריצה או אף במושגים של ערך כספי.

חשוב להדגיש כמו כן שעל אף קיומה של מערכת הצפנה יתכן מצב בו המחשב או המסוף או שניהם, מקרינים מידע גלוי בנוסף למידע שהוצפן. לכן, אותו גורם שמעונין לצותת יוכל להתרכז בהקלטת המידע הגלוי המשודר באותות חלשים נוסף למידע המוצפן. הטפול בהקרנות מעין אלו קשה ביותר וצבא ארה"ב לדוגמא, פיתח דרישות חמורות מציוד במגמה לעמוד בפני בעיות אלו. הדרישות הנ"ל מוגדרות במסגרת של עמידה במפרט TEMPEST.

ניתן למקם את ציוד ההצפנה באופנים שונים. מוכרות שלוש אפשרויות עיקריות של הצפנה. כמובן שמספר האפשרויות הנו בלתי מוגבל ויש לתכנן את ההצפנה של מערכת תקשורת נתונים בהתאם לדרישות מהמערכת וכן בשים לב להשקעות הכספיות של כל אפשרות. מפתח ההצפנה יכול להיות יחיד (SINGLE KEY ENCRYPTION) או מפתח ציבורי שבמקרה זה מתחלק לשני מפתחות (TWO KEY ENCRYPTION) או שלוב של הצפנה צבורית ושמוש במפתח יחיד.

האפשרויות הן כדלקמן :

א. בכל צד נמצא התקן הצפנה.

ב. מקרה דומה אולם כאן ההצפנה נעשית במחשב באמצעות תכנה. תכנה זו ניתן להתקין גם בקצה הקדמי (FRONT END) של המחשב שיעודו לטפל בתקשורת.

ג. הצפנת עורק שלם. כאן מרבבים לכתחילה יחד את כל המסופים המצויים במקום גיאוגרפי מסוים ולאחר מכן מצפינים אותם יחדיו. כמובן שכאן קיימת סכנת גלוי עד למרבב וכן המחיר של המצפן רחב הפס הוא גבוה יותר בדרך כלל מזה של מצפין קו יחיד.
יחד עם זאת נעשה כאן חסכון כולל של 2-ח מתקן ההצפנה.
(ח - מספר ציודי הקצה).

מגוון האפשרויות הינו גדול וחשוב לשקול היטב בכל מקרה לגופו של עניין.

נהול מפתחות הצפנה

נהול המפתחות מהווה גורם כבד ביותר של מערכת ההצפנה. חשוב ביותר לקבוע נוהלי עבודה ברורים של מועדי החלפת המפתחות.
אם כל המעורבים בתהליך אינם מחליפים מפתחות בו בזמן נקטעת אפשרות ההתקשרות. המפתחות עצמם חייבים להיות מוחזקים במקום מובטח פיזית אליו אין גישה פרט למוסמכים לכך. חשוב לקבוע גם את התהליך של העברת המפתחות אל סוגי הציוד השונים. עקרונית ניתן להעביר מפתחות פיזית ואף להטעינם מרחוק תוך שמוש בתקשורת נתונים (DOWN LOADING כאשר המדובר בהטענה ממחשב למסופים ו - UPLOADING כאשר מדובר בהטענה ממסוף למחשב). לעיתים גם חשוב לחלק את המפתחות כך שחלק יהיה בתוך התקן ההצפנה וחלק אחר בידי המשתמש (בדומה לנעשה במערכות הבנקאיות - בנקט, סניפומט וכדומה).

שיטות הצפנה בתקשורת נתונים

קיים מגוון גדול ביותר של שיטות הצפנה. על הגורם המתכנן לבחור את השיטה הנראית לו, כך שיקנה בטחון סביר למידע המועבר בשים לב לכלל המערכת הן מבחינת טופולוגיה, הרשויות בידיהן היא נמצאת, המחשבים וציוד הקצה. נזכיר כאן מספר שמות של שיטות בשמוש :

* שיטות שנוי מיקום (TRANSPOSITION).

* שיטות אלגבריות.

* שיטות החלפה (SUBSTITUTION).

* שיטת ההצפנה הציבורית (PUBLIC ENCRYPTION SYSTEM).

* שיטת תקן ההצפנה האמריקאי (DES - DATA ENCRYPTION STANDARD).

הצפנה צבורית

נבהיר כאן בקצרה את ההצפנה הצבורית לאור התאמתה לשמוש ע"י הצבור הרחב. ההצפנה הצבורית פותחה בשים לב לכך שיהיו שני מפתחות הצפנה. האחד מצוי במדריך גלוי והנו שייך לגורם אליו מעוניינים להעביר תשדורת מוצפנת. לכל אחד יש גישה למפתח זה וכל אחד יכול להשתמש בו אל הגורם הנ"ל. המפתח הזה משמש אך ורק להצפנה של המידע ולא ניתן באמצעותו לגלותו. המפתח לצרכי פענוח נמצא אך ורק אצל הגורם שאמור לקלוט את המידע. שיטה זו הידועה בשם RSA פותחה בשנת 1977 ע"י קבוצה של מדענים שעבדו ב - MIT (RIVEST, SHAMIR, ADLEMAN).
ניתן לשכלל את שיטת RSA גם ע"י הוספת אפשרות לזהוי (AUTHENTICATION). כאן השולח מעביר לקולט מפתח אישי שלו (שווה ערך לדוגמת חתימה בבנק), השולח מצפין את המידע קודם כל במפתח שלו ולאחר מכן תוך שמוש במפתח הצבורי. הקולט מפענח את ההודעה באמצעות מפתח הגלוי ולאחר מכן מזהה את המידע ע"י שמוש בפענוח נוסף לפי מפתח השולח המצוי בידיו.

הצפנה בתקן ההצפנה האמריקאי

הצפנה בתקן זה פותחה במגמה לאפשר עבודה בטוחה לגורמי הממשל האמריקאי. כיום ניתן להשיג התקנים אלו גם לגופים אחרים לאחר קבלת רשיון מתאים. תקן ההצפנה האמריקאי DES פותח בשים לב לכך שקיים מגוון רחב של מידע רגיש המועבר בתקשורת נתונים. מכון התקנים האמריקאי NBS - NATIONAL BUREAV OF STANDARDS חפש איפוא אלגוריתם תקני בו יעשה שמוש ע"י הסוכנויות הפדרליות האמריקאיות. התקן שנבחר היה לפי הצעה של חב' IBM שהבטיחה שמוש בתקן זה ללא הגבלות וללא תשלומים כלשהם לחברות האחרות היכולות לעשות בו שמוש ולמכור ציוד התואם תקן זה.

הקביעה שנעשתה בהקשר לתקן זה היתה כדלקמן :

"יש לממש את האלגוריתם של ה - DES לציוד מחשב או תקשורת נתונים תוך שמוש בטכנולוגיות חמרה. הממוש עצמו יכול להיות מותנה ביישומים, בסביבה ובטכנולוגיה שבשמוש. הממוש יכול להעשות תוך שמוש בפיסות עשויות LARGE SCALE INTEGRATION - LSI וכן התקנים בנויים מ - MEDIUM SCALE INTERGATION - MSI או התקנים אלקטרוניים אחרים המאפשרים ממוש האלגוריתם".

מכון התקנים האמריקאי הבטיח כמו כן לספק נוהלי בחינה לבדיקת עמידת הפיסות בדרישות ואף לבצע בחינות כאלה.

הצפנה של מערכות פתוחות

ניתן לממש מערכת הצפנה בכל אחת מהשכבות שמעל לשכבה הראשונה. יש להדגיש כי כאשר מצפינים שכבה מסויימת במערכת אחת, ניתן לפענח את המידע רק בשכבה זהה של מערכת העובדת מולה. ככל שההצפנה נעשית בשכבה גבוהה יותר כן גם מושג יותר בטחון מבחינת שמירה על הגישה אל המידע.

נסקור בקצרה את אפשריות ההצפנה בשכבות השונות :

* הצפנה בשכבת העורק (רמה 2) - יש צורך בהצפנה נפרדת בכל עורק ששייך למסלול הנתונים. את מצפיני העורקים ניתן להטעין מרחוק במפתח קריפטו מתאים או באופן ידני. אין מצפינים כאלה חייבים שנוי כלשהוא במחשב ו / או במסופים. המצפנים ברמת העורק משמשים במערכות תקשורת נתונים פשוטות המורכבות בדרך כלל מעורק יחיד.

* הצפנה בשכבת הרשת (רמה 3) - בשיטת הצפנה זו הנתונים המוצפנים מועברים דרך מספר עורקים מבלי שיש צורך לפענח את הנתונים לאחר כל עורק ולהצפינם מחדש. ההצפנה יכולה להעשות או בתוך ציוד תקשורת הנתונים או בתוך ציוד הקצה לתקשורת הנתונים. כאשר ההצפנה נעשית בתוך ציוד התקשורת לנתונים היא נעשית בפועל ברמת הרשת הצבורית או הפרטית. במקרה זה יש צורך במפתח קריפטו מיוחד לכל כתובת שמצריכה תקשורת מוצפנת. דבר זה מסבך במידה נכרת את הרשת אולם איננו מחייב שנויים בציוד הקצה לנתונים.

כאשר משתמשים בפרוטוקול X.25 ומעוניינים לבצע את ההצפנה בציוד הקצה לתקשורת נתונים, נתקלים בקושי וזאת משום שהפרוטוקול ברמה 3 של X.25 תומך רק בבקרת התקשורת בין המשתמש לרשת ואיננו תומך בתקשורת ממשתמש למשתמש. לכן, אין כל אפשרות לבצע כאן את ההצפנה.

* הצפנה בשכבת ההובלה (שכבה 4) - ניתן לממש מצפינים בשכבה זו בקצה הקדמי של המחשב או ישירות במחשב ובמסוף. בכל אופן, המסופים בהם נערכת הצפנה בשכבה זו חייבים להיות חכמים. מיקומה של ההצפנה בשכבה זו מביאה למעשה להצפנה מקצה לקצה. חייבים לשים לב היטב לכך שהצפנה בשכבה זו לא תמנע אפשרות הבנת הנעשה על ידי השכבות הנמוכות יותר. יש לכך איפוא תשלום גבוה בתכנה.

* הצפנה בשכבת המושב (שכבה 5) - בשכבה זו לא ניתן להבחין בין היישומים השונים שעשויים להיות מטופלים במסגרת המושב. לכן, הרווח הצפוי בהצפנה בשכבה זו נמוך בהשוואה להצפנה בשכבה 4.

* הצפנה בשכבת הייצוג (שכבה 6) - ההצפנה בשכבה זו מוגבלת לפרוטוקולי תקשורת שקופים וזאת משום שתווים מוצפנים שיופיעו כתווי בקרה יגרמו לבלבול בשכבות הנמוכות יותר. כאשר שכבת הייצוג נמצאת במעבד הקצה הקדמי או בבקר המסופים ניתן לממש בהם את פונקציות החמרה של ההתקנה. לחליפין, ניתן לממשו גם במחשב המארח או במסוף אם בתוכם ואם בהתקנים נפרדים. כאשר ממוש הצפנה בשכבה זו נעשה בתכנה, ניתן גם להתקין תכנה זו במחשב המארח או במסוף, או בקצה הקדמי ובקו התקשורת כפי שנאמר על ממוש בחמרה. כאשר פונקציות ההצפנה מצויות בשכבת הייצוג, ניתן להשתמש עבור מערכת הנהול של המערכת באותן אפשרויות החמרה והתכנה שמשמשות בהצפנת הקבצים.

* הצפנה בשכבת היישום (שכבה 7) - בשכבה זו מצפינים למעשה את המידע וזוהי הרמה הגבוהה ביותר של האבטחה. בדרך כלל נעשית היא בחמרה במחשב או במסוף. אפשר לבצע הצפנה זו גם בתכנה אם כי בארה"ב לדוגמא, אוסרת על כך הממשלה.

סכום

נושא בטחון המידע בתקשורת נתונים הנו בעל חשיבות עליונה ותוך שמוש נכון בו ניתן ליעל במידה רבה את השרותים הצבוריים והפרטיים.

מדי יום מתווספות שיטות חדשות ואלגוריתמים חדשים.

חשוב לשים דגש על נושא ההצפנה ולבחירה באופן מושכל.

תפקידי הנהלה וגורמים מקצועיים של הארגון בישום אבטחת מערכות ממוחשבות.

דן גרנות.

הרקע.

תוך חצי יובל עשה מחשב דרך ארוכה מכלי מעבדתי דרך היותו סמל יוקרה עד לסוס עבודה הכל יכול בשטח תקשוב ומערכות מידע.

השנים האחרונות מסמלות חדירת מערכות מידע ממוחשבות לרוב שטחי פעילות ארגונית של מוסדות וארגונים. נוספו וגוונו פונקציות ומשימות המתבצעות בעזרת תוכניות מחשב, גדל נפח מידע מאוחסן עם יכולת שליפה מהירה וסלקטיבית,למחשבים מרכזיים התווספו מסופים, מחשבים אישיים, או תחנות עבודה רבות המאפשרות בצוע חשובים וקבלת מידע אנליטי או גרפי מידי לכל צרכי הארגון. למעשה קרובים אנו לזמן בו מתגשמת האמרה של אסימוב מ 1978 "אנו לא מפחדים מהמחשבים, אנו מפחדים להשאר בלעדיהם".
היות ומגמת ההרחבה של מערכות ממוחשבות נמשכת בקצב מהיר יש יסוד להניח שבעתיד קרוב מאד יווצר מצב בו פגיעה רצינית במתקן המיצר או מאחסן מידע עצמו תגרום להאטה ובמקרים חמורים לשתוק מוחלט של פעילות מנהלית בארגון כולו. לאור האמור חיוני להתיחס ברצינות לסיכוני הפגעות של מתקני מחשוב ולחפש בעוד מועד פתרונות שיאפשרו אבטחה, גיבוי והתאוששות מהירים של שרותי מחשוב במקרה של נזק או פגיעה.

באשר המודעות להווצרות הסיכונים הוצורך להלחם נגדם החלה כבר לחדור להנהלות הארגונים, תהליכי נתוח הסיכונים, הערכת צרכים, מנגנון זיהוי אלטרנטיבות ובחירת פתרונות המועדפים וישומם, טרם פותחו במידה מספקת.
מטרת המאמר היא, להציע דרך לבצע תהליך בחירת הפתרונות ולהגיע להחלטות מוסכמות של כל הגורמים המעורבים בנושא אבטחת מידע ממוחשב, תוך התחשבות בדרישות ספציפיות ונצול מומחיות של כל אחד מן הגורמים האלה.

הפגעות מערכות ממוחשבות.

מערכות מידע ממוחשבות בארגון גדול מורכבות מאמצעים רבים ומגוונים (אנשים, חומרה, תוכנה, תשתית) ועלותם גבוהה. גם הסיכונים שבפניהם חייב מערך גיבוי להגן, הם מרובים ורבגוניים. כדי להשיג בצורה מסודרת ויסודית נתונים הדרושים לחיפוש פתרונות להגנה וגיבוי המערכים יש צורך לבצע תחילה נתוח סיכונים. מטרת ניתוח הסיכונים היא לסקור נכסי המערכת ואת הפגועים האפשריים בה, כדי לקבוע הפסד משוער מארועים מסוימים, על יסוד הסתברות מופע של אותם הארועים. הסתברות מופע בלתי רצוי, היא בדרך בכל פרופורציונלית הפוכה לעוצמתו. למשל שריפה רצינית עלולה לגרום לנזק של מליונים, אך הסתברות מופע שלה היא נמוכה מאד. מצד שני מחיקות מידע מקריות קורות הרבה, אך עלות הנזק שהן גורמות, היא קטנה. נתוח סיכונים מחייב רכוז סיסטמתי של נתונים אודות הסיכונים ומאמץ להעריך את הנזק אותו הם עלולים לגרום.
היעד של ניתוח הסיכונים הוא קבלת מידע אודות עלות שנתית של הנזק שעלול להגרם מסיכון בודד, קבוצת סיכונים ועלות הנזקים של כל המערכת. התוצאה של נתוח הסיכונים זה, יכולה גם לשמש כחסם לאשור הוצאה כספית, המיועדת לנקיטת אמצעים שיבטלו או יקטינו עד למינימום את הווצרות הסיכונים. ריכוז הסיכונים יקל גם על הכנת תכנית ארועים אפשריים (CONTINGENCY PLAN) היכולה לסייע בבצוע תרגולי התגוננות בפני פגיעות.

חפוש פתרונות.

שלב הבא הוא חפוש פתרונות, שיאפשרו הקטנת נזקים למערכות מידע, פגיעות פיזיות, תקלות טכניות או שגיאות אנושית ושיקצרו זמן החזרת מערכת חישוב הפגומה למצבה התקין. לכל אחד מסוגי הפגיעות יש פתרונות רבים שיוכלו להקטין או אולי למנוע לגמרי נזקים. פתרונות אלה נבדלים ביניהם בדרך בכל בשלמות הבצוע, זמן ועלות. ברור שהמצב האידיאלי הוא למצוא עבור כל סיכון את הפתרון הטוב ביותר, שיגיב במהירות ושיהיה גם זול מאד.

במציאות כל שפור בצועים עולה כסף ולכל ארגון ישנה מסגרת תקציבית שבמגבלותיה הוא פועל. עקב מגבלות התקציב ההנהלת הארגון רוצה ברוב המקרים לכסות מירב הסיכונים ולהבטיח רציפות מקסימלית של פעילות מערכות ממוחשבות, במינימום הוצאות. ברור שלצורך זה דרושה הכרות מעמיקה של הארגון, יעדיו האסטרטגיים, מבנהו, ותוכניותיו העתידות. ברור שידע זה אינו נמצא ואינו מוכר לגורם בודד אלה מפוזר בין פונקציות שונות כך שעבוד מידע זה חייב להתבצע רק בעבודת צוות.

אפיון הגורמים המעורבים באבטחת מידע ממוחשב.

כדי להמשיך בפתוח הנושא נבחון תחילה את כל הגורמים השותפים למשימה של אבטחת מידע ממוחשב. בדרך כלל בנושא אבטחת מידע ממוחשב מעורבות ארבעת פונקציות ארגוניות הבאות:

1. הנהלת הארגון.
2. צרכני מערכות מידע ממוחשבות.
3. מרכז החישוב.
4. גורמי ביטחון של הארגון.

ננסה עתה לאפיין כל אחת מפונקציות אלה ובמיוחד את התיחסותן לנושא אבטחת מידע ממוחשב.

הנהלת הארגון.

ההנהלה ברוב הארגונים מודעת לחשיבות המידע, שהפך בזמן האחרון למשאב ארגוני נוסף בהמשך למשאבים ארגונים המוכרים מקודם (כוח אדם, ציוד, חומרים, הון). בארגונים רבים הוקם נהול מקורות מידע (IRM INFORMATION RESOURCE MANAGEMENT אשר מספק להנהלה אלמנטים קריטיים של מידע.
אי לכך להנהלה יש ענין רב במידע ובשמירתו. מצד שני אנשי הנהלות הם בדרך כלל אנשים בעלי מקדם לקיחת סיכון גבוה יותר (תכונה זאת גם תרמה לעליתם לתפקידם הנוכחי) הם גם בדרך כלל אופטימיסטים באופים גם בנושא השרדות של מערכי מידע ממוחשב.

צרכני מערכות מידע ממוחשבות.

הצרכנים מודעים ברוב המקרים לחשיבותה של אבטחת מערכות מידע במסגרת תפקידם, הם מוכנים לתמוך העמדה זאת כל עוד אין זה דורש מהם להשקיע אמצעים (בצוע עבודה נוספת או השקעות בספיות). הצרכנים מאמינים ש "לי זה לא יקרה" ואינם נוטים לקבל המלצות, אותן שוללים בנמוקים של אי קיום אמצעים או חוסר אמון באשר לסבירות הסיכון.

מרכז החישוב.

תפקידם של אנשי מרכז החישוב הוא לפתח מערכים חדשים, לבצע שנוים ולתחזק מערכים הקיימים המשרתים את הארגון כולו. הם סובלים ממחסור כרוני של כוח אדם וכתוצאה מזה נמצאים תמיד בפגור בלוח בצוע המשימות שלהם. הם היו רוצים לשפר אבטחת מידע, להוסיף אמצעי חומרה ותוכנה נוספים למטרה זאת אך לעתים חוסר זמן לבצוע בדיקות של יעילות מוצרים אלה, התאמתם למערכות הקיימות ולפעמים גם חוסר תקציבים מונעים מהם בצוע משימות אלה.

גורמי בטחון של הארגון.

אנשי הביטחון של הארגון הם הגורם הרגיש ביותר בנושא אבטחת מידע, כאשר רובם מתעמקים במיוחד בשטח אבטחה פיזית ונאמנות אנשים. בזמן האחרון ישנה נטיה בארגונים מסוימים לקרב את אנשי בטחון גם לאמצעי אבטחת מידע בעזרת חומרה ותוכנה. גורמי בטחון ממקדים את הערכותיהם בדרך כלל במבט יחסית צר ורואים דברים במושגים של דרישות קבועות. גורמי הבטחון הם גם בדרך כלל שמרנים ונוטים בדרך כלל להמנע מלקיחת סיכונים. דרישות למגבלות של אבטחת מידע מגורמי הבטחון הן ברובן חד ערכיות אינן כוללות אלטרנטיבות שהיו משאירות להנהלה מרחב תמרון.

תהליך אבטחת מידע.

כדי לבחון ולי‍ישם תהליך אבטחת מידע ממוחשב חייבים לבצע את השלבים הבאים:

א. הגדרת הסיכונים האפשריים והספציפיים לארגון.
ב. הערכת הנזקים העלולים להווצר בתוצאה מהתגשמות הסיכונים.
ג. הצגת פתרונות אפשריים למניעה או להתגברות על הסיכונים.
ד. בחירת פתרונות אופטימלים וישומם.

כפי שראינו קודם, ארבעת הגורמים המעורבים בטפול בנושא אבטחת מידע ממוחשב הם בעלי השקפות ועמדות שונות במה שנוגע לישום תהליך אבטחת מידע. חלוקי דעות אלה עלולים לגרום לקשיים, עכובים וחוסר התקדמות, אך למעשה לכל אחד מן הגורמים ישנן סמכויות פורמליות בתחומים מסוימים, רקע וידע מקצועי חיוני להצלחת המשימה כולה. המטרה שעומדת בפנינו היא למצוא חלוקת סמכויות ותחומי עבודה שיאפשרו השגת שתוף פעולה מירבי עם נצול מקסימלי של כשורים מקצועיים בכל אחד מן השלבים שפורטו קודם.
דרך הפתרון היא לפי דעתינו נצול מוטיבציה, התמצאות מיקום פיזי ואחריות פורמלית של כל אחד מן הגורמים. גם תלקח בחשבון עוצמת מעורבות בשלב מסוים למשל גורם אחד ירכז הנושא וגורם אחר ישמש כגורם מסייע. ברור שלאחריות פורמלית יהיה משקל רב בקביעת אחריות בבצוע שלבים.

נבנה עתה טבלה המציגה את עוצמת וצורת השתתפות של גורמים שונים בבכל אחד מן השלבים של התארגנות אבטחת מידע ממוחשב.

פונקציה ארגונית / שלב בתהליך	הנהלת הארגון	צרכני מערכות	מרכז החישוב	גורמי ביטחון
תאור סיכונים האפשריים בארגון			סיוע מקצועי	רכוז הסקר
הערכת הנזקים האפשרים בארגון	בדיקת השלכות לטווח ארוך	בדיקת יכולת השרדות	רכוז מידע	בדיקת נזקים ביטחונים
הצגת פתרונות האפשרים בארגון		בדיקות התאמה לתהליכי עבודה	בדיקת יכולת ישום מקומי	
בחירת פתרונות אופטימלים וישומם	בדיקת כדאיות החלטה סופית		סיוע מקצועי	סיוע מקצועי

ברור שיכולים להיות הבדלים קלים בתוכן הטבלה עבור ארגונים שונים בהיותם בעלי יעוד, מבנה ארגוני והגדרות תפקידים שונות, אך העקרון המנחה הוא התאמת ידע מקצועי והתמכות של גורמים שונים לשלביה תהליך המתאימים.

שלב תאור הסיכונים האפשרים בארגון ירוכזו על ידי גורמי הביטחון בסיוע מקצועי של אנשי מרכז החישוב. אנשי ביטחון יבחנו במיוחד אספקטים של אבטחה פיזית, בקרת כניסות, נאמנות של בעלי תפקידים רגישים והתגוננות בפני אסונות טבע.
סיוע של אנשי מרכז החישוב יתבטא בבחינת סיכונים של חדירה למאגרי מידע ורשתות תקשורת.

בשלב הערכת הנזקים יש תפקיד חשוב לצרכני מערכות מידע. עליהם להעריך מידת יכולת השרדות במקרה של פגיעה במערכת, ולהעריך מידת הנזק שעלול להווצר עקב פגיעות במערכות שונות.הנהלת הארגון חייבת כאן לבחון מסקנות של הצרכנים ולצרף את ההשלכות של פגיעות לטווח ארוך, אשר בדרך כלל לא נלקחות בחשבון על ידי הצרכנים. מרכז החישוב בוחן השפעות הנזקים של חומרה ותוכנה והשפעתם על המערכת כולה, כאשר גורמי בטחון מתרכזים בבדיקת נזקים הנובעים מפגיעה בהוראות בטחון.

שלב החיפוש אחרי פתרונות מתבצע ברובו על ידי אנשי מרכז החישוב. הפתרונות חייבים להתאים לחומרה ותוכנה הקיימות, לקחת בחשבון תוכניות פתוח עתידות. נציגי צרכנים יסיעו בשלב זה על ידי בדיקה של התאמת הפתרונות לפעולות הצרכנים.

השלב האחרון מחייב נתוח כדאיות, החלטה סופית על בחירת פתרון מועדף ואבטחת תקציב לרכישת חומרה ותוכנה, במקרה של החלטה חיובית. כאן פעילות ההנהלה היא הדומיננטית, כאשר היא נעזרת ביעוץ מקצועי של אנשי מרכז החישוב וגורמי הבטחון.

דרך אחרת להמחשת מורכבות הבעיה, אולי בצורה יותר כללית היא בעזרת הנוסחה הבאה:

$$\frac{S \times E}{C} \cong \text{const.}$$

כאשר:

S = רמת אבטחת המידע במערך.

E = רמת יעילות ונוחיות הפעלה של המערך.

C = עלות פתוח ואחזקת המערך.

שפור רמת אבטחת מידע במערך משיגים בדרך כלל על חשבון יעילות ונוחיות הפעלת המערך ו/או על ידי הגדלת עלות הקמת, ואחזקת מערך המידע.

על שפור רמת אבטחת המידע נלחם גורם בטחוני. הצרכן בדרך כלל דואג לעלות ומרכז החישוב מעונין שהתוכנית אותה הוא מפתח תהיה יעילה ונוחה. הנהלת הארגון כגוף השולט על צרכני מערכות המידע, יחידת המחשב וגורמי הבטחון גם יחד, יכולה להוות גורם יחידי המסוגל לקבוע בצורה אוביאקטיבית את היחס הרצוי בין שלושת מרכיבים אלה.

סכום.

הכנסת שנוים הוא בדרך כלל תהליך קשה ומסובך, במיוחד כאשר מדובר במערכות דינמיות ואינטראכטיביות כמו מערכות מידע. ישום אבטחת מידע יעיל מחייב בצוע שנוים ארגוניים וטכנולוגיים בהם מעורבים אנשים רבים. חלוקי דעות וגישות שונות בין פונקציות ארגוניות קיימות גם בעבודה שגרתית, אך בשעת בצוע שנוים רמת חלוקי דעות עולה בהרבה. נראה לנו שהקצעת משימות ותפקידים בשלבים שונים של התארגנות לאבטחת מידע על ידי התאמת סמכוית הפונקציות לשלבי התהליך ונצול מירבי של התמכויות מקצועיות יכולה להבטיח סבירות גבוהה להצלחה במשימה.
דרך זאת של הקצעת משימות ותפקודים לאורך הזמן, תקל גם במידה מסוימת על קביעת משקל יחסי של כל אחד משלושת הגורמים שהוזכרו קודם.
(הצרכן, מרכז החישוב וגורמי בטחון). אך עדין יהיה צורך במעורבות רבה של הנהלה, כדי להתגבר על בעיות של רגש ויוקרה שהן המהוות את עיקר של אי הבנות. רק גישה פרגמטית של הנהלה המבוססת על בדיקה ענינית של עלות/תועלת תבטיח פתרון הוגן ויעיל.

אבטחת מידע במערכת S.W.I.F.T

ג'וני ירום
בנק לאומי לישראל בע"מ

חברת S.W.I.F.T הינה ארגון המספק שרותים לבנקים ומוסדות פיננסיים להעברת הודעות.

האמצעי המרכזי במתן שרותים אלה הינה מערכת תקשורת בינלאומית המבוססת על מחשבים המופעלת ע"י חברת S.W.I.F.T לטובת הבנקים החברים בה.

רשת התקשורת הינה יחודית ממערכות תקשורת ציבוריות אחרות, ב-2 אספקטים:-

א. רוב ההודעות המועברות ברשת הינן הודעות בעלות מבנה מובנה מראש. עובדה אשר חייבה את ההנהלה הבנקאית הבינלאומית לאמץ מבנה הודעות אלו ואשר הביא למינימום סיכונים והקטנת שגיאות בהודעות.

ב. רשת התקשורת נבנתה כך שאבטחת המידע בנויה בה כשיטה, המאפשרת אבטחת הרשת כנגד שינוי בין ע"י טעות ובין במתכוון.

שני אספקטים אלו הינם חשובים ביותר מאחר שחלק נכבד מההודעות העוברות ברשת התקשורת הינן העברות כספים.

מערכת S.W.I.F.T פועלת החל מאמצע שנות ה-70 ולכן גם תכנון הרשת ופילוספית השרות של המערכת תואמים את המוצרים של אותה תקופה.

הרשת פועלת באמצעות 3 מרכזי מחשבים גדולים הממוקמים בבלגיה, הולנד וארה"ב.

מרכזי מחשבים אלו מחוברים בקווי תקשורת למרכזי מחשבים האזוריים במהירויות של 9,600 באוד.

כעקרון קיים מרכז אזורי אחד לכל מדינה ומדינה.

ישנם כמובן מקרים חריגים כמו למשל בארה"ב לה 4 מרכזים אזוריים וכן מס' מדינות באירופה.
קיימת מגבלה של חיבור מס' בנקים למרכז אזורי אחד.
כל מרכז אזורי מקושר לאחד משלשת מרכזי מחשבים כאשר קיים קשר נוסף למרכז מחשבים נוסף, כאשר הקשר הנוסף משמש במקרים של נפילות של הקו הראשון.

כל בנק אשר הינו חבר במערכת מתחבר למרכז האזורי בקו תקשורת במהירויות של 4800/2400 באוד.
במקרים של נפילות קווים נעשה שימוש בקווי חיוג.

בכל בנק החבר ברשת קיימת מערכת מחשב השולחת ומקבלת הודעות.

חברת S.W.I.F.T העולמית מספקת חומרה ותוכנה לרשות הבנקים לשימושם במערכת.

מערכות המחשבים של הבנקים מספקות את השרותים הבאים: -

א. העברת הודעות לבנקים אחרים ברשת

ב. אפשרויות שיחזור הודעות שנעברו ברשת

ג. אפשרויות מיתוג הודעות למסופים המוגדרים מראש.

<u>הבנקים בישראל</u>

כל הבנקים אשר הינם סוחרים מוסמכים במט"ח שותפים לרשת S.W.I.F.T.

<u>אבטחת מידע במערכת</u>

במסגרת ההרצאה תוצג המערכת כולל אמצעי אבטחת המידע הננקטים בחומרה ובתוכנה של הרשת.

תקציר הרצאה

היבטים משפטיים (אזרחיים ופליליים)
בהפעלת מערכות מידע ממוחשבות

יצחק מלכו, עו"ד - רח' חובבי ציון 8, ירושלים

המשפט הוא מטבעו בעל אופי שמרני ואילו הטכנולוגיה היא מעצם מהותה יציר חדשני; לכן, מידי פעם מתקשה המשפט למצוא פתרונות משבעי-רצון לתוצאות הנובעות מיישומם של פיתוחים טכנולוגיים, או להשפעותיהן.

אחד הנושאים הבולטים בהם כללי המשפט עדיין אינם מסוגלים להעמיד פתרונות מספקים לתוצאות יישומה של פריצת-דרך טכנולוגית, הוא הנושא של "מערכות מידע ממוחשבות".

התהום הפעורה בין ההישג הטכנולוגי המרשים, שהושג בשנים האחרונות בפיתוח מערכות מידע ממוחשבות, לבין כללי המשפט המסורבלים העומדים לרשותנו לצורך הטיפול בתוצאות ובהשפעות - של יישומו בחיינו, מקבלת ביטוי בכמה וכמה ענינים, המעוררים סוגיות הן בתחום המשפט האזרחי והן בתחום המשפט הפלילי.

להלן ניתוח מקוצר של כמה ענינים מיוחדים נבחרים כאלה, אשר קשורים, באופן כזה או אחר, גם בתחום ההתענינות של משתתפי הכינוס הנוכחי, היינו: "בטיחות מערכות מידע".

1. האחריות להפצת מידע מוטעה

סוגית האחריות להפצת מידע ממוחשב שיש בו שיבוש או טעות בלתי מכוונים, עשויה להתעורר, לענייננו בקרות אחד האירועים האלה: תקלה במאגרי המידע הממוחשב, חדירת מידע מוטעה מטעם ספק מידע חיצוני למאגר המידע הממוחשב, תקלה בקווי התקשורת המחברים את מאגר המידע הממוחשב עם המסוף של מבקש המידע הסופי.
בכל אחד מהמקרים הללו ראוי להטיל את האחריות המשפטית לתוצאות השיבוש או הטעות על גורם אחר, וזאת - בין היתר - בהתחשב בסוג המידע בו מדובר ובמיהות המבקש המעונין להשתמש במידע.

2. הפצת "לשון הרע" במערכות מידע ממוחשבות

סוגיה זו עשויה להתעורר, לענייננו, כאשר הממונים על הפעלתה של מערכת מידע ממוחשבת עושים בה שימוש גם לצורך העברתן של ידיעות, המסופקות למאגר המידע של המערכת על-ידי ספק מידע חיצוני (כגון: מערכות העיתונים היומיים), אשר יש בהן תוכן העלול להחשב כמשמיץ. והשאלה היא, האם ראוי להטיל במקרה כזה גם על הממונים על הפעלת מערכת המידע הממוחשבת אחריות כמי שפורסמו דבר לשום הרע, למרות שהמערכת שימשה רק כצינור להעברת המידע המשמיץ ותו לא.

3. <u>ההגנה על זכויות יוצרים במידע הנצבר במאגרי מידע ממוחשבים</u>

סוגיה זו עשויה להתעורר, לעניננו, באותם מקרים בהם האחראים על מערכת מידע ממוחשבת מעוניינים לאגור בה מידע שיש לגביו זכויות יוצרים לגיטימיות לאחרים (למשל: ערכים שלמים מתוך האינציקלופדיה בריטניקה), ואח"כ להעביר את המידע הזה למסופים של מבקשי מידע העשויים להתענין בחומר הנאגר כאמור. כאן, עיקרו של הקושי הוא בכך שאגירת המידע במאגר הממוחשב ואף העברתו אל מבקשי המידע נעשים באמצעים מגנטיים-דיגיטליים ולא בדרכים הרגילות של העתקה המוכרות לחוקי זכויות היוצרים והנאסרות על-פי הוראותיהם.

4. <u>ההגנה מפני חשיפת מידע פרטי המצוי במאגר מידע ממוחשב</u>

אין זה מתקבל על הדעת שהמשפט יאפשר לעשות שימוש לרעה ביכולת העצומה הגלומה במערכות מידע ממוחשבות לרכז מידע אודות הפרט. לפיכך, סוגיה זו הוסדרה במשפטנו, כמו במשפטי יתר מדינות המערב, באמצעות דבר חקיקה של המחוקק הראשי, (חוק הגנת הפרטיות, תשמ"א-1981) ותיקון תקנות ע"י מחוקק המשנה. וכמו דברי חקיקה אחרים, המיועדים לטפל בהסדרת הפעלתם של אמצעים טכנלוגיים מורכבים, גם החוק והתקנות הללו לוקים בחסר ובמיותר.

5. <u>גניבת תוכנה ומידע מעובד</u>

אחד היסודות ההכרחיים על מנת להרשיע אדם בעבירת גניבה, לפי המשפט הפלילי שלנו וגם לפי משפטן של יתר המדינות העוקבות אחר שיטת המשפט האנגלית, בהתאם לפרשנות השמרנית המקובלת, הוא כי הנאשם "יטול" באופן פיסי "דבר" כלשהו (שוב במובן הפיסי) השייך למישהו אחר.

מובן מאליו, שעל-פי הפרשנות המקובלת הזאת, נטילת תוכנה או מידע מעובד - גם אם ערכם הכלכלי רב - לא תוכל להחשב כגניבה אם אלה "נלקחו" באמצעים אלקטרוניים, על-ידי חדירה באמצעי תקשורת של בעל המחשב המענין אל תוך המאגר הממוחשב בו מצויים התוכנה או המידע המעובד המהווים את אובייקט "הלקיחה".

הדרך האפשרית להקנית משמעות פלילית ולהטלת עונש בשל מעשי "לקיחה" מן הסוג הזה, כפולה היא.

האחת, ע"י פרשנות - שיש בה מידה לא קטנה של תעוזה - של יסוד "הנטילה" האמור בעבירת הגניבה ככולל גם "נטילה אלקטרונית", ולא רק נטילה פיסית רגילה;

והשניה, שהיא הדרך המועדפת בעיני, ע"י חקיקת חוק שיגדר עבירה חדשה, הלוא היא "עבירת המחשב", המוכרת כבר בחקיקתן הפלילית של מדינות רבות.

פונקציות הבקורת בסביבה ממוחשבת, הווה ועתיד - תקציר

המרצה - ששון מרון-מועלם.

כפי שהכרנו בעבר, הדיספלינה (discipline) של הבקורת היתה,הערכה של הפעילות הפיננסית של הפירמה בתקופה קודמת.

בעת הופעתם של מערכות מחשבים והתרחבות השימוש בהם בפירמות,התברר, כי תהליך עיבוד הנתונים לא צמצם את הצורך של בקרה פנימית במערכת.נהפוך הוא,נראה יותר מתמיד שיש צורך לשים דגש על בחינת קיום הבקרה כדי לוודא שהיא יעילה במערכות מתוחכמות כאלה.

כידוע , יעילותה של הבקרה במערכת נמדדת עפ"י התרומה שלה ל:

- גילוי ומניעת טעויות.
- גילוי ומניעת מעילות ותרמיות.
- מניעת עיבוד כפול של נתונים ומצביעה על מצבים של אובדן נתונים.
- מניעת אובדן של נתונים כאשר חלק מהמערכת נפגם ומאפשרת שיחזור בעת הצורך.

השימוש במחשב לעבוד נתונים, היה נחוץ, ובא לענות על צרכים ודרישות השעה של המשתמשים.

מרכוז העסקים מצד אחד וביצוע עבודים בתפזורת מצד שני הגדיל את הדרישות להספקת מידע כדי לענות על אספקטים נהוליים ותפעוליים , כגון:

דרישות לעיבוד מידע לצרכי דווחים חשבונאיים , פיסקליים , כלכליים , תמחיריים ועוד.

הזיקה למידע גדלה , כיון שכל הדווחים הנ"ל התבססו על מסות גדולות של נתונים שנוצרו בארגונים וריכוזם בשיטות העבודה הידניות שהיו מקובלות , נעשה בלתי אפשרי.

המידע הינו התוצאה של עבוד הנתונים הנ"ל.

התוצאה הישירה והעיקרית היא שהמידע בארגון הפך להיות נכס אסטרטגי , נכס עיקרי שבלעדו לא מתאפשר המשך קיום הארגון.

מידע זה סופק כמובן באמצעות המערכות לעבוד הנתונים.

בעקרון , למידע צריך שיהיו ה תכונות הבאות: שלם , עדכני , נכון , אמיתי , משקף אל נכון , ניתן להתבסס עליו לצורך קבלת החלטות.

כדי להבטיח את התכונות הללו למידע , נוצרו מערכות הבקרה שהמבקרים הם חלק מהם .

בראשית כניסת המחשבים לשימוש בעולם העסקים , המבקרים החלו לבצע בקורת מסביב למחשב. אולם בעת שנוכחו שבעקבות השימוש במחשב חל כירסום בראיות הבקורת ונתיבי בקורת שהיו אפשריים לפני עידן השמוש במחשב (כמו למשל בקרות ארגוניות ונוהליות) , הצטמצמו , הגיעו למסקנה שכדי לקיים

את המוטל עליהם כמתחייב מהוראות מקצועיות , נחוץ בדחיפות להכיר , להבין ולהיות מודעים לתהליכים ולציוד של עבוד נתונים אוטומטי , במטרה להשיג מומחיות לבקורת מערכות כאלה כדיספלינה חדשה.

הקונספציה יושמה פחות או יותר בהצלחה ברוב פונקציות הבקורת הפנימית , אולם יישום זה היה כרוך בקשיים , כי השנויים יצרו בעיות חדשות, התווספו פונקציות חדשות לבקורת, נקבעו והונהגו נהלים ויישומים חדשים.

בארגונים /פירמות גדולות שהשתמשו במערכות מחשב גדולות, מבקרי פנים החלו להשתמש במחשב לעזרת הבקורת. שוב הדבר לא היה קל , כי פונקציות הבקורת נתקלו בציוד שונה ותוכניות שונות לאפליקציות במחלקות.

בשל מורכבות הפעולות, מורכבות המערכות, ריבוי התוכנות ואפשרויות היישומיות של הציוד, המשתמשים נזקקו לעזרת הבקורת. המבקרים נקראו לייעץ להנהלות אירגוניהם בטרם החליטו לרכוש ציוד, בעת עיצוב מערכת וכתיבת תוכניות. על אף המגבלות של הסטנדרטים המקצועיים, כמו אי התלות והאובייקטיביות, המבקרים נאלצו להחלץ לעזרת המשתמשים בשלב העיצוב או התכנון כדי לוודא שהבקרות היעילות אכן תשובצנה בתוכנות.

בענין זה המבקרים לא יכלו לדחות את המשתמש בטענה "כי זה באחריותך, תעשה ואחר כך תראה לנו",כי עלות השנוי הינה גבוהה ביותר.

בין השינויים הצפויים שתהיה להם השלכה על עתיד הבקורת, ניתן לציין:

א) פתוחים חדשים בציוד, בעיקר צפויים לחזות בהופעתם של מיקרו-מחשבים עם זכרון גדול. וכתוצאה מכך הרחבת העבודים בתפזורת.

ב) פתוחים של מכשירי הקלט יאפשרו קליטת הנתונים באמצעות דיבור במקום לוח מקשים.

ג) פתוחים של תוכנות מתוחכמות , מערכות מתוחכמות יאפשרו לימוד עצמי.

ד) שפות תכנות פשוטות יאפשרו רישום תכניות בקלות.

ה) התפתחות השימוש בתוכנות אפליקציה בקשת רחבה יותר של ציוד.

ו) פתוח רשתות תקשורת בין מחשבית.

כל זה אולי זעיר אנפין של פתוחים שעתידים לבוא , זה יהיה עולם עתיר טכנולוגיה ועתיר מידע. ובעולם זה תפקיד המבקר יהיה יותר מורכב, יותר קשה, יחייב הכשרה והתמחות מתמדת.
המבקרים צריכים להיות מסוגלים להעריך באופן ריאלי את הסיכונים במערכות עיבוד הנתונים ואת היעילות של הבקרות בתוכניות אפליקציות שונות , בקרות הקלט ובקרות הפלט, בקרות גישות ובטיחות הנתונים במערכת, לרבות אמצעי התקשורת.
לצורך זה על המבקרים יהיה לפתח טכניקות בקורת חדשות וכמובן להסתייע בטכניקות כאלה המבטיחות קיום בקרות באמצעות המחשב. זה מחייב השקעת משאבים, הכשרת אנשים והתמחות כדי שיוכלו להיות יועצים מוצלחים להנהלות ארגוניהם, כמתחייב מהאחריות המקצועית בעידן פתוח טכנולוגי מעולה.

אין ספק כי בעתיד יתגברו ציפיות ההנהלות מהמבקרים, לגבי בחינת נאותות נהלי הבקרה ובאיזה מידה הם עוזרים להשיג את מטרות הארגון.
ההנהלות ודאי יצפו מהמבקרים להכיר ולהבין את המערכות לעבוד נתונים אוטומטי שהן תומכות את הפעילות העסקית , כחלק אינטגרלי של עבודת הבקורת.

כדי שהמבקרים יצליחו לענות לציפיות , אני סבור, בין היתר , כי הלשכות המקצועיות יוכלו לסייע בכוון זה. הסיוע צריך לבוא לידי ביטוי בהכוונה בעזרת סטנדרטים והנחיות מקצועיות , וכמוכן בקביעת תוכניות הכשרה מותאמות לדרישות הבקורת בפרקטיקה.

APPLIED ARTIFICIAL INTELLIGENCE: EXPERT SYSTEMS - THE FUTURE OF INFORMATION SYSTEMS SECURITY, EDP AUDITING AND CONTROL

Raoul Pollak,
President,
BMB Security Knowledge
Systems Limited,
P.O.Box 126, GIVATAYIM
ISRAEL 53101.

A B S T R A C T

This Position Paper indicates that the direction in which future Information Systems Security and EDP Auditing measures and techniques should develop, is in the field of Applied Artificial Intelligence : Expert (Support) Systems and Expert Systems.

Computers and related technologies are being developed at an unprecedented speed.

The Information Systems Society suffers serious damages and losses from large-scale Computer Crime, Industrial Espionage and Terrorism. These threats and vulnerabilities will increase and reach techno-terrorism levels endangering, also, high-tech installations.

Present I.S. Security measures and EDP Auditing and Control techniques are inadequate in order to cope with the rapid technological changes in a vulnerable environment.

The transition from present security methods and auditing techniques will be gradual. Basic Security concepts, Control objectives and EDP Auditing techniques will continue to function. But, crucial tasks and burdens for security and audit of the future Information Systems will fall on Expert Systems.

Present vulnerabilities and Future technological developments are reviewed. A Meta-Knowledge Base for I.S. Security and a Meta-Knowledge Base for EDP Auditing are presented. Main components of Expert System Building Stages are indicated. Four Expert Systems for Risk Analysis, Crisis Management, Disaster Recovery and Personnel Security, are reviewed. Directions for future development of Expert Systems in the field of I.S. Security and EDP Auditing are outlined.

EXPERT SYSTEMS FOR INFORMATION SYSTEMS SECURITY, AUDITNG AND CONTROL

A. FROM EXPERT SYSTEM TO EXPERT SUPPORT SYSTEMS

"Expert Systems are often thought of as systems that can replace human experts. For most business applications, the knowledge that can be feasibly encoded in an expert system is not sufficient to make satisfactory decisions alone. Instead, the focus should be on designing Expert Support Systems that will aid, rather than replace, human decision makers."

Artificial intelligence Expert Systems will not replace computer security officers nor EDP Auditors, but will assist them in executing their difficult tasks more efficiently, quicker and punctually. Expert Systems help security officers and Auditors in the decision making processes in complex situations where time factors are critical, such as decisions in crisis management and on-line EFT auditing.

B. THE FUTURE OF EDP AUDITING AND CONTROL

"The fifth generation will stand apart, not only because of its technology, but also because it is conceptually and functionally different from the first four generations. The new machines will be known as "Knowledge Information Processing Systems"(KIPS). The question is: "How will KIPS be controlled?" Are their functions auditable by human beings? How can "symbolic manipulation" be audited and "automated reasoning" be controlled?

Only several years ago, managers had to substitute manual auditing for Electronic Data Processing (EDP) auditing after they finally realized that "auditing around the computer" did not bring results. EDP Auditors then had to struggle to gain recognition as members of the committees supervising software development teams, in order to introduce EDP controls during the System Development Life Cycle (SDLC).

Soon after learning to control the program's changes, written in high-level structural languages, a new problem arose: How to use a Data Dictionary/Directory System for auditing purposes. A year or so later, with the introduction of the fourth generation languages, which enabled programming by endusers, the EDP auditors realized that the convenient multi-stage SDLC had disappeared and turned into a simple Systems Analyst-Enduser relationship. A new auditing challenge then arose: How to audit the fourth-generation (non-structural) application programs developed by endusers.

At present, the microcomputer revolution and micro-mainframe communication insecurity pose new problems and challenges for auditors. How can millions of micros be audited and controlled? With change in technology, auditors' skills change too. The non-EDP Auditor has already been phased out. EDP Auditors who were only yesterday struggling with techniques of auditing large mainframe Data Base Management Systems (DBMS) are today looking for techniques and solutions to audit micro DBMS in network environments. Will the EDP profession survive with the advent of the fifth generation? One prediction says auditors will be replaced by software engineers, specializing in auditing.

If so, how safe will the fifth generation be? Who will exercise control? Will it take fifth-generation computers to audit and control fifth-generation computers? Or will a computer audit itself with some inbuilt logical controls? How vulnerable will society be in case of failure? How vulnerable will fifth-generation computer-managed factories, traffic, hospitals, banks and offices, be in case of arson, terrorist attack, fraud, techno-terrorism or espionage?

How good will these machines be at syping on us? Will they also be used to spy on one another? Will we be able to control them or will we eventually become controlled by them? Who will control the fifth-generation controllers? Is a new ruling "computer controller class" emerging?

The answers are difficult. Partial solutions lie with the development of Expert Systems in the field of I.S. Security and EDP Auditing and Control.

C. THE SIX BASIC RULES FOR FUTURE SECURITY AND AUDITING TECHNIQUES

The future of any Security System (including Information System Security) and EDP Auditing lies with Expert Systems. This statement is based on six basic rules:

1. Computer Technology is moving more rapidly than computer security officers and EDP Auditors can control, without Expert Systems.

2. Fourth generation systems cannot be audited with (present) third generation software.

3. Endusers' micro-computer driven computing, networking and large mainframe systems can be secured satisfactorily only with Expert Support Systems.

4. The future of Information System Security and EDP Auditing and Control lies with Expert Systems, because of technical deficiencies in our present methods for Security Auditing and Control.

5. Only Expert Systems can secure, audit and control other Expert Systems.

6. An Expert System may have, in itself, elements of a self-Auditing and Control System. They can also explain the basis for their conclusions ("Audit Trail").

D. THE FUTURE FIELDS OF I.S. SECURITY EXPERT SYSTEMS

Security Expert Systems will be rapidly developed in the following fields:

1. RISK ANALYSIS EXPERT SYSTEM
   - based on the CRITICAL - SURVIVAL - FACTOR - DRIVEN method.
2. DISASTER RECOVERY EXPERT SYSTEM
   - Expert Systems for Crisis Management and Disaster Recovery. The 'FIPREX'' Expert System for Fire Fighting
3. DISASTER RECOVERY EXPERT SYSTEM
   - for High-Tech and I.S. Security installations and production facilities.
   - for fighting chemical contamination from Technoterrorists (TERROREX)
4. 4-LEVEL (MINI - MICRO - MAINFRAME - NETWARE)
   - Distributed Contingency Planning Expert Systems.
5. PERSONNEL SECURITY AND INVESTIGATION EXPERT SYSTEM
   - (SAPEX)
6. INSURANCE EVALUATION AND DECISIONS SUPPORT SYSTEM
   - (INSUREX)

E. FUTURE EXPERT SYSTEMS IN THE FIELD OF EDP AUDITING

Emanating from technological changes Large Vulnerability and Management Problems , the Future EDP Auditing will need Expert Systems in the following fields:

1. Auditing loan allocation - in banking.
2. Collateral control - in banking.
3. Data Base Auditing.
4. Network Auditing.
5. Auditing Fourth Generation Development. The traditional SDLC has changed. User driven computing caused the Audit Trail to vanish. In the complex System Analyst-Enduser relationship, only logical Expert System Controls will have real practical value.
6. Auditing micro-computer access to mainframe files.
7. Expert Systems for Auditing as stand-alone systems.
8. Expert Systems for Auditing the Information Centre.
9. Expert Systems combined with SMF(System Management Facilities) on large scale IBM Systems, for auditing purposes.

הבקורת הפנימית ובטיחות המידע

שלמה הנדל - C I S A
אגף הבקורת הפנימית-בנק לאומי לישראל בע"מ

הצורך באבטחת מידע לא נולד עם חדירת המחשבים לארגונים. הוא היה קיים גם קודם אך, הגורמים שהביאו לכך שתהליכים הקשורים במערכות מידע ימוסדו ויאורגנו חשיבתית ותורתית, הם אלה אשר פעלו גם על תחום אבטחת המידע.
תהליכים אלו אשר השפיעו על הארגון בכללותו, לא פסחו על הבקורת הפנימית.

הצהרת אחריות הבקורת הפנימית מגדירה את מטרות והיקף הבקורת תחת חמשת ההגדרות הבאות:-

1. סקירת המהימנות והשלמות של מידע פיננסי ותפעולי ושל אמצעים בהם משתמשים כדי לזהות, למדוד, לסווג ולדווח מידע כזה.
2. סקירת המערכות שנקבעו כדי לוודא בצוע המדיניות, התכניות, הנהלים, החוקים והתקנות אשר להם עשויה להיות השפעה משמעותית על פעולות ועל דוחו"ת, וכדי לקבוע אם הארגון פועל בהתאמה.
3. סקירת האמצעים לשמירת נכסים, ולפי הצורך, אימות קיומם של נכסים אלה.
4. הערכת השמוש הכלכלי והיעיל במשאבים.
5. סקירת פעולות או תכניות כדי לוודא באם התוצאות תואמות את המטרות והיעדים שנקבעו, ובאם הפעולות או התכניות מבוצעות כפי שתוכנן.

בקורת בסביבה ממוחשבת גרמה למערכות הבקורת הפנימית, כמו למערכות הנהול, לצורך בהתאמה של המסגרות התורתיות לסביבה החדשה על בסיס הסטנדרטים המקצועיים המקובלים.

מכיון שהמידע הוכר כמשאב או נכס רב ערך וחשיבות, בעצמה גדולה בהרבה עם חדירתם של המחשבים, הרי שהתמקד הצורך "לסקור את האמצעים לשמירת המידע" (הנכס) ולפי הצורך לאמת קיומו. זאת כמובן, בנוסף לשאר המשמעויות המצויות בהיקף הבקורת כגון: סקירת מהימנות ושלמות המידע, הערכת שמוש כלכלי ויעיל במידע ועוד.

בעבר, כתולדה מזיהוי מאוחר יחסית של המידע כנכס, ומאי-קיומם של אמצעים סבירים לשמירתו, נוצר מעין חלל אשר זוהה על-ידי גורמי הבקורת. בהעדר המודעות בארגון ובהעדר מנגנון נהולי ותפעולי נאות, פעלה הבקורת בשטח האבטחה. הדבר קבל את בטויו במקרים מסויימים בהרשאת גישה שאושרו על-ידי הבקורת. מצב זה גרם לפגיעה בעקרון אי-התלות והאובייקטיביות של המבקר.

במשך הזמן אותר בארגונים הצורך בהקמת מנגנון בקרה תפעולי שתפקידו לשלוט על הגישה והשמוש במידע ולבקרם.

מרחב הפעולה של הבקורת הפנימית מקיף את בחינת והערכת הלימותה ויעילותה של מערכת הבקרה הפנימית בארגון ואת טיב הבצוע של התפקידים שהוטלו.

אבטחת המידע הוא "מנגנון בקרה" אחד מיני רבים, וככזה, הינו באחריות ההנהלה וחותך את ההגדרות שאוזכרו.

הקשר הנכון בין הבקורת לפונקציית אבטחת המידע, צריך שיתבצע בדומה לגישת הבקורת למנגנוני נהול, ובקרה אחרים.

על הבקורת לסקור תקופתית את קיומו, דרך נהולו ועצמתו של המנגנון.

על-פי תוצאות הסקירה תקבע הבקורת הפנימית את מידת ועומק מעורבותה בהיבטים של אבטחת מידע בעת הבקורות השוטפות שהיא עורכת על מרחב הפעילויות.

בתהליכי היום-יום, יש קשר הדוק בין הבקורת הפנימית ופונקצית אבטחות המידע בתחום הגדרת הכללים והמסגרות ולעתים כפועל יוצא מתוצאות עבודת הפונקציה המחייבות התיחסות של הבקורת מתוקף תפקידה ומעמדה המקצועי.

קשר חשוב זה צריך בניה מושכלת תוך שמירה על מרקם המסגרות בארגון.

תיכנון למצבי חרום

דגנית אמתי

מהנדסת - מערכות, חברת רד"ט

מרבית הארגונים תלויים כיום יותר ויותר בתיפקוד מערך מחשבים. מערך זה הכולל מידע, חומרה, תוכנה, תיקשורת ואנשים חשוף לאיומים ולסכנות שאין לחזותם מראש, העשויים לגרום לשיתוקו החלקי או המוחלט.

ככל שגוברת התלות במערך המחשבים, כך גדל הנזק העלול להגרם לאירגון כולו כתוצאה מפגיעה במערך המחשבים, נזק אשר יכול להוביל לחסולו של האירגון.

ההכרה בתמונה - מצב זו ובחומרתה הובילה בשנים האחרונות, להתפתחותן של מתודולוגיות "תיכנון לשעת חרום" (CONTINJENCY PLANMIMG). מטרתן של מתודולוגיות אלה היא להתוות קווי-פעולה למקרה אסון מתוך כוונה לצמצם ככל האפשר את מימדי הנזק.

בהרצאתי אסקור את הגישה המסורתית כפי שהיא משתקפת במתקני-מחשבים.

כפי הגישה המקובלת, "תיכנון החרום" הוא תהליך ההגדרה, הפיתוח והתעוד של תוכנית חרום אשר תופעל מיד לאחר התרחשות אסון, שבעטיו לא יכולים שרותי המיחשוב של הארגון לתפקד במתכונתם הרגילה.

מקובל לראות את התהליך כמושתת על המרכיבים הבאים:

א. ניתוח סיכונים.

ב. קביעת יישומים קריטיים חיוניים.

ג. הגדרת תצורת חומרה מינימלית.

ד. ניתוח אפשרויות הגיבוי.

ה. הכנת תוכנית פעולה.

ו. ניסוי וביקרות.

סקירת הגישה המקובלת חושפת נקודות תרופה וקשיי יישום הפוגמים במטרה הסופית. כמענה לקשיים אלה מוצעת תפיסה אירגונית - ניהולית מחודשת המאוחדת כנקודת מבט הגדרה שונה של המושגים אסון ותקלה, מתוך מטרה לקרוא לגישת ניהול המשלבת את תיכנון החרום כחלק מניהול התקלות וההתאוששות השוטף של המתקן.